Impact of IPSec mode on Performance and Security

Lin Chen, Kitty
NYU Tandon School of Engineering
NY, USA
klc616@nyu.edu

Abstract - Internet Protocol Security (IPSec) is a standard for securing internet communication and, a widely deployed mechanism for implementing remote connection between devices in a WAN or LAN. This paper presents the performance analysis of the Tunnel mode vs Transport mode configurations. The results show a negligible difference in speed even though Tunnel mode offers better protection against network attacks.

INTRODUCTION

With the advent of the Covid-19 pandemic, companies have been forced to adopt remote work arrangements with unexpected speed. This has exposed cyber security weaknesses within many organizations, and forced them to adopt more stringent measurements to prevent further breaches. There are already many security tools and processes available like VPN and IPsec tunnels, but their proper configuration and performance have become crucial to ensure the protection of all the stakeholders.

IPsec (Internet Protocol Security) is a framework designed to protect IP traffic on the network layer. IPsec can protect traffic with the following features:

- Confidentiality: by encrypting our data, nobody except the sender and receiver will be able to read our data.
- Integrity: we want to make sure that nobody changes the data in our packets. By calculating a hash value, the sender and receiver will be able to check if changes have been made to the packet.
- Authentication: the sender and receiver will authenticate each other to make sure that we are really talking with the device we intend to.
- Anti-replay: even if a packet is encrypted and authenticated, an attacker could try to capture these packets and send them again. By using sequence numbers, IPsec will not transmit any duplicate packets.

IPsec supports two main modes: transport mode and tunnel mode. In our research we will investigate and compare the efficiency and security of both configurations.

OVERVIEW OF IPSEC

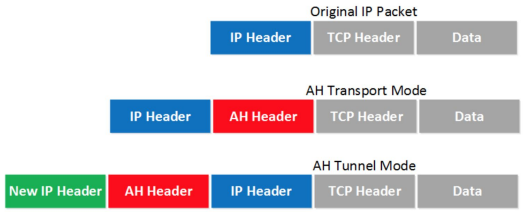
IPsec makes use of tunneling. The data packets that we define sensitive or interesting are sent through the tunnel securely. By defining the characteristics of the tunnel, the security protection measures of sensitive packets are defined. IPsec offers numerous technologies and encryption modes. But its working can be broken into five major steps. A brief overview is given below:

- Interesting Traffic Initiation: the sensitive traffic that needs to be monitored is deemed interesting. After deciding about the traffic, the security policy is implemented on the configuration interface for the peers.

- IKE Phase One: in this step, first the IPsec peers are authenticated thus protecting the identities of the peers. Then the Internet Key Exchange (IKE) Security Associations (SA) policy is negotiated among the peers. This results in both the parties to have a shared secret matching key that helps in the IKE phase two.
- IKE Phase Two: this phase negotiates information for IPsec SA parameters through the IKE SA. Here as well IPsec policies are shared and then establish IPsec SAs. There is only a single mode (quick mode) in this phase. It exchanges nonce providing replay protection. These nonces generate new shared secret key material. If the lifetime for IPsec expires, it can renegotiate a new SA.
- Data Transfer: here the data is safely and securely transmitted through the IPsec tunnel. The sent packets are encrypted and decrypted using the specified encryption in the IPsec SAs.
- Tunnel Termination: the tunnel may terminate by either deletion or by time out.

TUNNEL MODE VS TRANSFER MODE

The main difference between the two is that with transport mode the original IP header is used, while in tunnel mode, a new IP header is used. The difference is illustrated below:



Transport mode is often used between two devices that want to protect some insecure traffic. Tunnel mode is typically used for site-to-site VPNs where we need to encapsulate the original IP packet since these are mostly private IP addresses and can't be routed on the Internet. With tunnel mode, NAT traversal is supported and because additional headers are added to the packet, MSS (TCP Maximum Segment Size) is smaller. With transport mode, NAT traversal is not supported, but MSS is higher.

Tunnel mode seems to be the safer configuration for nowadays cybersecurity needs, and even recommended for device to device communications. By encapsulating the original IP packet, we can prevent attacks like IP spoofing. The latency may be higher since MSS is smaller but the trade-off may be worth it. However, for intensive activities like video and multimedia transmissions, the performance overhead compared to transport mode might dissuade the user from adopting a more secure configuration.

RELATED RESEARCH

A study on the overhead of IPSec using a bare PC softphone showed that considering processing overhead, tunnel mode was only slightly more expensive than transport mode. The overhead increase percentage for incoming versus outgoing packets was largest for ESP without authentication in tunnel mode, and smallest for ESP with either authentication option in transport mode [1]

Another study of the impact of IPSec on interactive communications showed that, provided an infrastructure with adequate bandwidth, the influence of IPSec was not noticeable by the user. The already small differences in the network metrics were not detectable in the perceptual quality anymore. [2]

In our study we'll compare the performance of Strongswan IPSec under the tunnel mode vs transport mode. We'll measure the speed of packet transmission by pinging the other side of the tunnel. Packet transmission

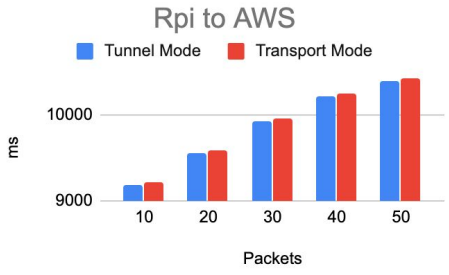
speed under tunnel mode is expected to be slightly slower but with negligible impact on performance.

METHODOLOGY AND ANALYSIS

In our research we measured the speed of packets transmission by setting up a raspberry pi 4 with Ubuntu installed on it and connecting it to an AWS EC2 server via an Ipsec tunnel. We installed Strongswan libraries on both ends and tested two configurations of the tunnel: transport mode and tunnel mode. We used the ping command to measure the speed of transmission of packets of different sizes. Figure 2 shows a slightly higher overhead in transport mode compared to tunnel mode. The packet sizes correspond to durations ranging from 9000 to 11000 ms. The difference between configuration modes was about 30 ± 5 ms and increased linearly with the packet size. The difference may be negligible when used with real time applications but it may not apply to users with lower bandwidth internet connections.

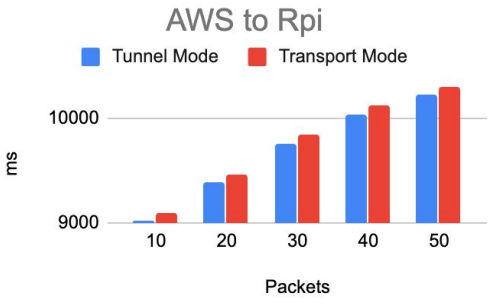
Rpi to AWS ping:

Packets	Tunnel Mode (ms)	Transport Mode (ms)
10	9174,0	9208,0
20	9541,0	9576,3
30	9922,6	9959,4
40	10220,3	10258,2
50	10424,7	10463,3



AWS to Rpi:

Packets	Tunnel Mode	Transport Mode
10	9014,0	9087,0
20	9374,6	9450,5
30	9749,5	9828,5
40	10042,0	10123,4
50	10242,9	10325,8



Conclusion

Security is a highly discussed topic nowadays, and protocols like IPSec and VPN are becoming more and more frequently used to secure communications in our workplaces. The aim of this research was to bring a detailed view of the performance of data transmission over an IP-based network. We compared the speed of data transmission between IPSec in tunnel mode vs transport mode. The measured results demonstrated a negligible speed impact over a high bandwidth network. It showed that regardless of the increased overhead caused by the additional layer of encryption in tunnel mode, its performance is on the same level as IPSec transport mode, but more secure.

REFERENCES

[1] Evaluation of IPsec Overhead for VoIP using a Bare PC. N. Kazemi, A. L. Wijesinha, and R. Karne.

Department of Computer and Information Sciences. Towson University. Towson, MD 21252

[2] On the Impact of IPsec on Interactive Communications. Jirka Klaue, Andreas Hess. Technical University Berlin

[3] Internet Protocol Security (IPSec) Mechanisms. Hani Alshamrani. International Journal of Scientific & Engineering Research. 2014